AMENDMENTS

Please amend the application as follows:

In the Specification:

Please amend Paragraph [0015] as follows:

In the on-line commercial transaction process, a customer using a customer terminal 104 is connected to an open network 106 such as the Internet. The customer terminal 104 is preferably a personal computer at use in a home or office. It should be understood that the customer terminal 104 may be any digital device that can be communicably connected to an open ~~network.106~~ network 106 and is capable of receiving data input by the customer and processing the data input by the customer before transmission to the open network 106.

Please amend Paragraph [0028] as follows:

To make the HSM 114 compliant with X9 requirements, the programmed HSM 114 requires that private keys and symmetric keys exist [[inn]] in an acceptable secure format. The keys may be rendered as cleartext inside the protected memory of a tamper resistant security module, or encrypted when rendered outside of the protected memory of a tamper resistant security module. The keys may be rendered as two or more key fragments or key components either in cleartext or ciphertext and managed using dual control with split knowledge fragmentation of the keys. Secret-sharing enables the key fragments to be stored separately on tokens so that less than all of the key fragments (k-of-n key fragments) are required to load or reconstitute the key being protected. Good security practice requires key separation, whereby

each key or key pair is generated for a particular purpose and used solely for the purpose for which it was intended.

Please amend Paragraph [0030] as follows:

The HSM interface 110 may be encased [[inn]] in a durable, tamper-resistant casing to safeguard the system against incursion. The HSM interface 110 should also include built-in detection techniques capable of sensing sophisticated attempts at physical or electronic tampering. These techniques may provide for immediate and automatic erasure of secured algorithms and data stored in the device.

Please amend Paragraph [0043] as follows:

The secure PIN processing system 100 relies on the HSM 114 not just for security but [[by]] also to insure the cryptography which is CPU intensive is optimized for high scalability and is capable of supporting diverse applications. The secure PIN processing system and process 100 may dramatically increase the number of cryptographic keys generated, distributed, installed, used, and eventually terminated. This proliferation will stress the scalability of key management software and the key storage mechanisms that will be forced to manage more and more cryptographic keys.

Please amend Paragraph [0055] as follows:

The transaction module generates a transaction message including transaction data and corollary data at function block 338. Proceeding to function block 340, the transaction module ~~send~~ sends the transaction message to the transaction manager 102. The transaction manager sends the dynamic data and algorithms and the corollary data to the HSM interface 110 at function block 342. The HSM interface 110 injects the HSM dynamic data and algorithms, seed data and corollary data to the HSM 114 at function block 344. Proceeding to function block 346, the HSM 114 calculates the customer PIN, based on the algorithms, seed data and corollary data. The HSM 114 encrypts the PIN using an injected key-encryption-key at function block 348. The HSM 114 may encrypt the PIN using any of a variety of encryption techniques. In accordance with the preferred embodiment, the encryption is performed using a dual-controlled, split-knowledge key, which has been injected into the HSM 114 using a smart card 116. The HSM 114 then generates a PIN block using the encrypted PIN at function block 350.